UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/610,798	07/06/2000	Suresh Krishna	BRCMP003	4877

28393 7590 02/03/2004

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVE., N.W.
WASHINGTON, DC 20005

EXAMINER	
ORTIZ, BELIX M	

ART UNIT	PAPER NUMBER
2175	17

DATE MAILED: 02/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/610,798	KRISHNA ET AL.	
	Examiner	Art Unit	
	Belix M. Ortiz	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-23 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-23 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 06 July 2000 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a)☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3,10-14 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the drawings: character "124", in page 8, line 21 and character "204", in page 11, line 1, are not shown on the drawings. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

2. Applicant is required to submit a proposed drawing correction in reply to this Office action. However, formal correction of the noted defect may be deferred until after the examiner has considered the proposed drawing correction. Failure to timely submit the proposed drawing correction will result in the abandonment of the application.

Specification

3. Heading appears underlined throughout the disclosed specification.

Heading should not be underlined.

4. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-7, 9-17, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barlow et al. (U.S. patent 6,038,551) in view of Markham (U.S. patent 5,796,836).

As to claim 1, Barlow et al. teaches a cryptography acceleration chip (see column 11, lines 43-47), comprising:

a plurality of cryptography processing engines (see column 7. lines 42-45); and

a packet distributor unit configured to receive data packets and matching classification information for the packets, and to input each of the packets to one of the plurality of cryptography processing engines (see column 17, lines 58-67; column 18, lines 1-8);

Barlow et al. does not teach wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order.

Markham teaches a scalable key agile cryptography (see abstract), in which he teaches wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order (see abstract; column 4, lines 7-10; column 11, lines 49-52).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al., to include wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al. by the teaching of Markham, because wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order, would enable the cryptography acceleration chip to provide key agility and placed in parallel will increase throughput through the encryption circuit. Failure to preserve the order of the cells will result in a loss of cryptographic synchronization (see Markham, abstract; column 4, lines 4-6; column 4, lines 21-23; column 11, lines 39-41).

As to claim 2, Barlow et al. as modified teaches wherein said distributor unit processes received packet and matching classification information sequentially (see Barlow et al., column 17, lines 59-66).

As to claim 3, Barlow et al. as modified teaches wherein said plurality of cryptography engines process the input packets in parallel (see Markham, abstract; column 4, lines 7-10; column 11, lines 49-52).

As to claim 4, Barlow et al. as modified teaches wherein said distributor unit inputs packets to the cryptography engines in round-robin fashion (see Markham, column 11, lines 5-6).

As to claim 5, Barlow et al. as modified teaches wherein said distributor unit reads packets output from the cryptography engines in the same round-robin fashion (see Markham, column 11, lines 21-25; column 11, lines 36-41; and column 12, lines 63-66).

As to claim 6, Barlow et al. as modified teaches wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a plurality of packet flows in parallel while maintaining packet ordering across the plurality of flows (see Markham, figures 11a, 11b, and 7a; column 11, lines 55-59).

As to claim 7, Barlow et al. as modified teaches wherein said packets require IPSec cryptography processing (see Barlow et al., column 2, lines 63-67; column 3, lines 1-13; column 5, lines 66-67; column 8, lines 27-29).

As to claim 9, Barlow et al. as modified teaches wherein said distributor unit further comprises an order maintenance retirement unit configured to enable the plurality of cryptography engines to process incoming packets in out-of-order fashion (see Markham, column 11, lines 39-41).

As to claim 10, Barlow et al. as modified teaches wherein said order maintenance retirement unit extracts processed packets from a retirement buffer and outputs them from the chip in the same order in which they were received by the chip (see Markham, column 11, lines 36-41).

As to claim 11, Barlow et al. teaches a method for accelerating cryptography processing of data packets (see column 11, lines 43-47), the method comprising:

processing the data packets and matching classification information for the packets (see column 9, lines 66-67 and column 10, lines 1-19).

Barlow et al. does not teach receiving a plurality of data packets on a cryptography acceleration chip;

distributing the data packets to a plurality of cryptography processing engines for cryptographic processing;

cryptographically processing the data packets in parallel on the plurality of cryptography processing engines; and

outputting the cryptographically processed data packets from the chip in correct per flow packet order.

Markham teaches a scalable key agile cryptography (see abstract), in which he teaches receiving a plurality of data packets on a cryptography acceleration chip (see column 11, lines 5-11);

distributing the data packets to a plurality of cryptography processing engines for cryptographic processing (see column 3, lines 58-66);

cryptographically processing the data packets in parallel on the plurality of cryptography processing engines (see column 4, lines 4-6); and

outputting the cryptographically processed data packets from the chip in correct per flow packet order (see column 4, lines 22-26).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al., to include receiving a plurality of data packets on a cryptography acceleration chip;

distributing the data packets to a plurality of cryptography processing engines for cryptographic processing;

cryptographically processing the data packets in parallel on the plurality of cryptography processing engines; and

outputting the cryptographically processed data packets from the chip in correct per flow packet order.

It would have been obvious to a person having ordinary skill in the

art at the time the invention was made to have modified Barlow et al. by the teaching of Markham, because receiving a plurality of data packets on a cryptography acceleration chip;

distributing the data packets to a plurality of cryptography processing engines for cryptographic processing;

cryptographically processing the data packets in parallel on the plurality of cryptography processing engines; and

outputting the cryptographically processed data packets from the chip in correct per flow packet order, would enable the cryptography acceleration chip to provide key agility and placed in parallel will increase throughput through the encryption circuit. Failure to preserve the order of the cells will result in a loss of cryptographic synchronization (see Markham, abstract; column 4, lines 4-6; column 4, lines 21-23; column 11, lines 39-41).

As to claim 12, Barlow et al. as modified teaches wherein said processing of received packet and matching classification information is done sequentially (see Markham, column 3, lines 63-66).

As to claim 13, Barlow et al. as modified teaches wherein said cryptographic processing of said packets on said plurality of cryptography engines is done in parallel (see Markham, figure 7a; column 4, lines 4-6; column 11, lines 55-59).

As to claim 14, Barlow et al. as modified teaches wherein said distribution of packets to the cryptography engines is done in round-robin fashion (see Markham, column 11, lines 3-6).

As to claim 15, Barlow et al. as modified teaches wherein said outputting of packets from the cryptography engines is done in the same round-robin fashion (see Markham, column 11, lines 21-25; column 11, lines 36-41; column 12, lines 63-66).

As to claim 16, Barlow et al. as modified teaches wherein, the combination of said distribution and cryptographic processing further maintains packet ordering across a plurality of flows (see Markham, figures 11a, 11b, and 7a; column 11, lines 55-59).

As to claim 17, Barlow et al. as modified teaches wherein said packets require IPSec cryptography processing (see Barlow et al., column 2, lines 63-67; column 3, lines 1-13; column 5, lines 66-67; column 8, lines 27-29).

As to claim 22, Barlow et al. teaches a network communication device (see column 7,lines 16-24), comprising:

a central processing unit (see figure 3; column 7, lines 16-17);

a system memory (see figure 3; column 7, lines 45-48);

a network interface unit (see column 7, lines 19-27);

a cryptography acceleration chip comprising (see figure 3):

a plurality of cryptography processing engines (see column 7, lines 42-45); and

a packet distributor unit configured to receive data packets and matching classification information for the packets, and to input each of the packets to one of the plurality of cryptography processing engines (see column 17, lines 58-67; column 18, lines 1-8);

an internal bus that connects the central processing unit, the system memory, the network interface unit, and the cryptography acceleration chip (see figure 3).

Barlow et al. does not teach wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order.

Markham teaches a scalable key agile cryptography (see abstract), in which he teaches wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order (see abstract; column 4, lines 7-10; column 11, lines 49-52).

Therefore, it would have been obvious to a person having ordinary

skill in the art at the time the invention was made to have modified Barlow et al., to include wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al. by the teaching of Markham, because wherein the combination of said distributor unit and plurality of cryptography engines is configured to provide for cryptographic processing of a plurality of the packets from a given packet flow in parallel while maintaining per flow packet order, would enable the cryptography acceleration chip to provide key agility and placed in parallel will increase throughput through the encryption circuit. Failure to preserve the order of the cells will result in a loss of cryptographic synchronization (see Markham, abstract; column 4, lines 4-6; column 4, lines 21-23; column 11, lines 39-41).

As to claim 23, Barlow et al. as modified teaches wherein the internal bus is a high speed switching matrix (see Barlow et al., figure 3, character 58).

7. Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barlow et al. (U.S. patent 6,038,551) in view of Markham (U.S. patent

5,796,836) as applied to claims 1-7, 9-17, and 22-23, and further in view of Krawczak et al. (U.S. patent 5,796,744).

As to claims 8 and 18, Barlow et al. as modified, still does not teach wherein said chip operates at sustained rate of at least one Gigabit/s in full duplex mode.

Krawczak et al. teaches multi-node interconnect topology with nodes containing SCI link controllers and gigabit transceivers (see abstract), in which he teaches wherein said chip operates at sustained rate of at least one Gigabit/s in full duplex mode (see column 1, lines 43-45; column 2, lines 12-21).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al., as modified, to include wherein said chip operates at sustained rate of at least one Gigabit/s in full duplex mode.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al. as modified, by the teaching of Krawczak et al., because wherein said chip operates at sustained rate of at least one Gigabit/s in full duplex mode, would enable the chip to achieve long distance high-speed packet transmission.

8. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Barlow et al. (U.S. patent 6,038,551) in view of Markham (U.S. patent 5,796,836)

and further in view of Krawczak et al. (U.S. patent 5,796,744) as applied to claims 8 and18 above, and still in view of Wasilewski et al. (U.S. patent 5,870,474).

As to claim 19, Barlow et al. as modified, still does not teach the method further comprising managing the processing of the packet data through the plurality of cryptography processing engines without requiring any attached local memory.

Wasilewski et al. teaches method and apparatus for providing conditional access in connection oriented, interactive networks with a multiplicity of service providers (see abstract), in which he teaches the method further comprising managing the processing of the packet data through the plurality of cryptography processing engines without requiring any attached local memory (see figure 2c, character 154, where "the plurality of cryptography" is read on "Des block").

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al., as modified, to include the method further comprising managing the processing of the packet data through the plurality of cryptography processing engines without requiring any attached local memory.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al. as modified, by the teaching of Wasilewski et al., because the method further comprising

managing the processing of the packet data through the plurality of cryptography processing engines without requiring any attached local memory, would enable the method of accelerating cryptography to work at higher speed, because splitting the packet into smaller fixed-size "cells", make it possible to process the cells in a predictable time frame and the cells may be fetches ahead of time and the pipeline may be staged in such a manner that the need for attached local memory is minimized.

9. Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barlow et al. (U.S. patent 6,038,551) in view of Wasilewski et al. (U.S. patent 5,870,474).

As to claim 20, Barlow et al. teaches An IPSec cryptography acceleration Chip (see figure 3), comprising:

an external system bus interface unit (see column 11, lines 30-32);

a packet classifier unit (see column 10, lines 20-39):

a packet distributor unit (see column 17, lines 59-65);

Barlow et al. does not teach a FIFO input buffer connected to the packet classifier unit;

a FIFO output buffer connected to packet distributor unit;

a plurality of cryptography processing engine units connected to the packet distributor unit; and

a control processor that manages the processing of packets through the chip.

Wasilewski et al. teaches method and apparatus for providing conditional access in connection oriented, interactive networks with a multiplicity of service providers (see abstract), in which he teaches a FIFO input buffer connected to the packet classifier unit (see figure 2c);

a FIFO output buffer connected to packet distributor unit (see figure 2c);

a plurality of cryptography processing engine units connected to the packet distributor unit (see figure 2c); and

a control processor that manages the processing of packets through the chip (see column 20, lines 5-7; column 20, lines 48-59).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al., to include a FIFO input buffer connected to the packet classifier unit;

a FIFO output buffer connected to packet distributor unit;

a plurality of cryptography processing engine units connected to the packet distributor unit; and

a control processor that manages the processing of packets through the chip.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Barlow et al. by the teaching of Wasilewski et al., because a FIFO input buffer connected to the packet classifier unit;

a FIFO output buffer connected to packet distributor unit;

a plurality of cryptography processing engine units connected to the packet distributor unit; and

a control processor that manages the processing of packets through the chip, would enable the cryptography acceleration chip by the control processor to communicate the information to the packet encryption processor via port, so that the processor can selectively control the encryption of program bearing transport packets. The classifier unit and distributor unit verifies the packet information and distributes the packet data through the plurality of cryptography processing engines, on the chip for security processing.

As to claim 21, Barlow et al. as modified teaches the IPSec cryptography, acceleration chip (see Barlow et al., figure 3), further comprising:

a packet splitting unit, in which incoming packets are split into fixed-sized cells (see Barlow et al., column 16, lines 63-66).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 703-305-7605. The examiner can normally be reached on moday-friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 703-305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

bmo

January 22, 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100